Docket No.: 2004P00922

CERTIFICATION

I, the below named translator, hereby declare that: my name and post office address are as stated below; that I am knowledgeable in the English and German languages, and that I believe that the attached text is a true and complete translation of PCT/EP2005/050453, filed with the European Patent Office on February 2, 2005.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Hollywood, Florida

Rebekka Pierre

September 7, 2006

Lerner Greenberg Stemer LLP
P.O. Box 2480
Hollywood, FL 33022-2480
Tel.: (954) 925-1100
Fax.: (954) 925-1101

1 Tamper-proof generation of true random numbers

2

3 The present invention relates to a method and an apparatus for

4 generating a true random number.

5

6 For access protection or encryption purposes, for example, it

7 is necessary to generate good tamper-proof random numbers. In

8 connection with vehicle immobilizers, said random numbers are

9 generated e.g. at engine control system level which in many

10 cases involves an embedded system, the use of external sources

11 being ruled out because of possible tampering and the use of

12 special circuits being ruled out due to the associated

13 additional piece costs.

14

15 One known method of generating true random numbers is to use

16 the low-order bits of an A/D conversion of signals from a

17 separate noise source. However, this entails considerable

18 costs. It is likewise known to generate a true random number

19 via a time measurement of an external event, e.g. the duration

20 of a key depression performed by the user. However, this

21 solution is ruled out at least in cases where the system

22 initiates communication and therefore has to generate the

23 random number prior to an external event. In addition to the

24 generation of true random numbers it is further known to use a

25 pseudorandom number sequence and store the current status e.g.

26 in a nonvolatile memory of the system. However, the quality of

27 pseudorandom numbers is unsatisfactory compared to true random

28 numbers.

29

30 The object of the invention is to specify a method and an

31 apparatus enabling a true random number to be generated

32 quickly, i.e. in the millisecond range, for example, in a

33 memory saving manner, independently of equipment runtime,

1 without storage between the operating cycles of the control

2 device and without external sources (random triggers).

3

4 This object is achieved by the features of the independent

5 claims.

6

7 Advantageous embodiments and developments of the invention will

8 emerge from the dependent claims.

9

10 The method according to the invention builds on the generic

11 prior art in that the true random number is generated on the

12 basis of a stochastically distributed duration of an electrical

13 charge reversal process. This solution produces a true random

14 number, i.e. not a pseudorandom number. Moreover, the method

15 cannot be manipulated by external circuitry. In many cases no

16 additional components compared to the existing configuration of

17 the relevant system are required, so that the additional costs

18 are minimal. A further advantage of the method according to the

19 invention is that it is not necessary to store a state which

20 could then be manipulated or rather reset. The inventive method

21 is particularly advantageous if the charge reversal process

22 constituting the stochastic source can be performed in a

23 component which is in any case an integral part of the system

24 which has to generate the random number as well as performing

25 other functions.

26

27 In preferred embodiments of the method according to the

28 invention it is provided that the charge reversal process

29 involves charge reversal of at least one memory cell. Memory

30 cells are an integral part of modern systems anyway and

31 therefore constitute a particularly cost-effective basis for

32 carrying out the charge reversal process.

33

1   In this connection it can be provided, for example, that at
2   least one memory cell is an EEPROM memory cell. The duration of
3   a charge reversal process of an EEPROM memory cell is subject
4   to comparatively large stochastic variations on the basis of
5   which true random numbers can be generated.
6
7   Alternatively, it is likewise possible for at least one memory
8   cell to be a FLASH memory cell. FLASH memories are being
9   increasingly used and therefore in many cases provide a
10 suitable basis for the inventive generation of true random
11 numbers without additional costs.
12
13 In preferred embodiments of the method according to the
14 invention it is further provided that the charge reversal
15 process is performed using a charge pump. Charge pumps are
16 commonly employed for example in connection with EEPROMs, on-
17 chip charge pumps being provided in many cases.
18
19 With the method according to the invention, it can additionally
20 be advantageously provided that the stochastic duration of the
21 charge reversal process is determined using a counter, it being
22 advantageous if the clocking of the counter is as high as
23 possible so that maximum variations are produced at the end of
24 the charge reversal process in respect of the count used as the
25 basis for the random number.
26
27 The method according to the invention is considered to be
28 particularly advantageous if provision is made for it to be
29 performed by an embedded system, in particular by an engine
30 control system of a motor vehicle. In such a case, all embedded
31 systems that are used in environments in which the generation
32 of good random numbers is (also) required are essentially
33 suitable.
34

1 The apparatus according to the invention builds on the generic

2 prior art in that it generates the true random number on the

3 basis of a stochastically distributed duration of an electrical

4 charge reversal process. This produces the advantages and

5 characteristics explained in connection with the method

6 according to the invention in an identical or similar manner,

7 for which reason reference is made to the corresponding

8 foregoing comments in order to avoid repetitions.

9

10 The same applies mutatis mutandis to the advantageous

11 developments of the inventive apparatus set forth below,

12 reference being made, in this regard also, to the corresponding

13 comments in connection with the method according to the

14 invention

15

16 The apparatus according to the invention is advantageously

17 developed in that it has at least one memory cell which

18 undergoes electrical charge reversal in order to generate the

19 random number.

20

21 It can be advantageously provided that at least one memory cell

22 is an EEPROM memory cell.

23

24 It is additionally or alternatively possible that at least one

25 memory cell is a FLASH memory cell.

26

27 The apparatus according to the invention is advantageously

28 developed by having a charge pump for performing the charge

29 reversal process.

30

31 In connection with the apparatus according to the invention it

32 can be additionally provided that it has a counter for

33 recording the stochastically distributed duration of the charge

34 reversal process.

1

2 Embodiments of the apparatus according to the invention wherein

3 it is provided that the apparatus is an embedded system, in

4 particular an engine control system of a motor vehicle, are

5 considered to be particularly advantageous.

6

7 An essential basic idea of the present invention is that true

8 random numbers can be generated virtually without additional

9 system costs if a component forming part of the system anyway

10 is used, such as a charge pump which is an integral part of a

11 control unit. The invention is particularly suitable for all

12 agencies having to generate a good, true random number using

13 existing systems (i.e. without specially provided components),

14 without having access to independent, tamper-proof generators

15 (triggers). These include, but are not limited to, in

16 particular all cost-optimized embedded systems. In the context

17 of automotive engineering, random numbers are required in

18 particular e.g. for access protection (including maintenance

19 work) and for encryption purposes (e.g. vehicle immobilizers).

20

21 Embodiments of the invention will now be explained by way of

22 example with reference to the accompanying drawings, in which:

23

24 Figure 1   is a flowchart illustrating an embodiment of the

25   method according to the invention;

26

27 Figure 2   is a graph showing possible charge reversal

28   processes of a memory cell;

29

30 Figure 3   shows a greatly simplified schematic block diagram

31   of components of an engine control system.

32

33 The embodiment of the inventive method illustrated in Figure 1

34 begins at step S1. In step S2 a counter is reset whose

1 subsequent count serves as the basis for generating the true

2 random number or which directly constitutes said random number.

3 In step S3 a charge reversal process is commenced and the

4 counter simultaneously started. The charge reversal process can

5 be in particular a write to an EEPROM or FLASH memory cell

6 which generally takes place using a charge pump. In step S4 it

7 is checked whether the charge reversal process is complete

8 until this is the case. Then in step S5 the counter is stopped.

9 In step S6 the count is read out and used as a true random

10 number. If necessary, however, the final random number can also

11 be generated using another computing function. The method shown

12 ends with step S7.

13

14 Figure 2 shows three stochastically distributed charge reversal

15 processes of a memory cell. The actual duration of a current

16 charge reversal process can be between a shortest duration T'

17 (curve Q') and a longest duration T'' (curve Q'') and can be,

18 for example, T (curve Q).

19

20 Figure 3 shows a highly simplified schematic block diagram of

21 engine control components, the engine control system 18

22 illustrated being present in the form of an embedded system.

23 The engine control system 18 can incorporate a large number of

24 other components (not shown) which are necessary for performing

25 all the tasks placed on the engine control system. All the

26 components explained in greater detail below are an integral

27 part of the engine control system 18 anyway, i.e. not specially

28 provided for generating the true random numbers. The engine

29 control system 18 shown has an intelligent controller 20 which

30 is suitable among other things for driving a charge pump 14

31 which is provided in order to reverse the charge of a memory

32 cell 10 of a memory cell array 22 of an EEPROM 12 when the

33 contents of the memory cell 10 are to be changed. The

34 controller 20 additionally communicates with a counter 16 with

1 which the actual duration of a charge reversal process of the

2 memory cell 10 is recorded. The average person skilled in the

3 part will recognize that, using the components shown in Figure

4 3, the method explained with reference to Figure 1 can be

5 carried out in an advantageous manner. The sequence of

6 generating a random number will not therefore be explained

7 again here.

8

9 The features of the invention disclosed in the above

10 description, in the drawings and in the claims may be essential

11 to the implementation of the invention both individually and in

12 any combination.

13